ПОЛИТИКА БЕЗОПАСНОСТИ

МУНИЦИПАЛЬНОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОД КРАСНОДАР «ДЕТСКО - ЮНОШЕСКИЙ ЦЕНТР»

1. АННОТАЦИЯ

Настоящая Политика безопасности в Муниципальном бюджетном образовательном учреждении муниципального образования город Краснодар «Детско-Юношеский центр» (далее – Политика) разработана для использования работниками Муниципального бюджетного образовательного учреждения муниципального образования город Краснодар «Детско-Юношеский центр» (далее – МБОУ ДО ДЮЦ) с целью усиления защиты информационно-телекоммуникационной инфраструктуры, в информационных системах персональных данных (далее – ИСПД) МБОУ ДО ДЮЦ, минимизации рисков несанкционированного доступа и снижению финансовых рисков, связанных с Политикой безопасности. Целевой пользователь документа – работники МБОУ ДО ДЮЦ.

2. ТРЕБОВАНИЯ

Все правила в области Политики безопасности, применяемые в МБОУ ДО ДЮЦ, при работе (сборе, обработке и хранении) с ИСПД включают соблюдение всех требований, установленных Положением МБОУ ДО ДЮЦ о персональных данных, о порядке обработки ИСПД работников МБОУ ДО ДЮЦ и гарантиях их защиты. Работники предупреждены, что не имеют права разглашать сведения третьим лицам о (об):

- фамилии, имени, отчестве;
- дате и месте рождения;
- гражданстве;
- паспорте (номер, дата выдачи, кем выдан);
- адресе места жительства (по паспорту, фактический), дата регистрации по месту жительства;
- номере телефона (домашний, сотовый);
- сведений о знании иностранных языков;
- образовании (наименование учебного заведения, год окончания, документ об образовании, квалификация специальность), профессии: стаж работы (общий, непрерывный, дающий право на выслугу лет);
- семейном положении;
- составе семьи (степень родства (ближайшие родственники, Ф.И.О. родственников, год их рождения);
- сведений о воинском учѐте;
- сведений о состоянии здоровья, необходимые работодателю для определения пригодности для выполнения поручаемой работы и предупреждения профессиональных заболеваний, предусмотренные действующим законодательством Российской Федерации;
- содержании заключѐнного контракта или трудового договора;

- сведений об аттестации, повышении квалификации, профессиональной переподготовке;
- сведений об использованных отпусках;
- сведений об имеющихся наградах (поощрениях), почѐтных званиях;
- сведений о номере и серии страхового свидетельства государственного пенсионного страхования;
- сведений об идентификационном номере налогоплательщика.

Работники МБОУ ДО ДЮЦ предупреждены, что в случае разглашения сведений, касающихся ИСПД, или их утраты несут ответственность в соответствии со ст. 90 ТК РФ.

Все правила в области политики безопасности, применяемые в МБОУ ДО ДЮЦ, в случае их регламентации, при генерации (создании) новых парольных фраз должны быть оптимизированы с учетом следующих требований:

− парольные фразы системных учетных записей (администратора домена, локального администратора, пользователя и т.д.) должны изменяться ежеквартально;
− запрещается передача парольных фраз пользователям при помощи почтовых сообщений либо иным открытым способом через Интернет. Открытый способ – такой способ передачи, при котором информация, попавшая к третьему лицу, может быть прочитана без использования парольной или криптографической информации;
− запрещается записывать свой пароль на бумаге, в файле, мобильных средствах и других носителях информации, в том числе на предметах. А также хранение его на рабочем месте;
− запрещается использовать для хранения хэша паролей алгоритм Microsoft LAN Manager (LM);
− парольная фраза учетной записи пользователя, имеющего административные привилегии, полученные при помощи членства в группе или при помощи программ, должна быть отличима от других парольных фраз учетных записей данного пользователя;
− при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях символов;
− все парольные фразы пользователей, а также системные парольные фразы должны соответствовать правилам сложности образования (создания, генерации) паролей.

Правила сложности образования паролей включает следующие положения:
− при образовании парольных фраз следует учитывать, что: парольные фразы должны содержать не меньше одного спецсимвола (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./), буквы в различном регистре и цифры; пароль не должен

включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;

− недопустимо хранение парольных фраз в доступном для любых третьих лиц виде;

− длина парольной фразы должна составлять не менее 8 символов.

3. ТРЕБОВАНИЯ К ПЕРЕДАЧЕ ПАРОЛЬНО-КЛЮЧЕВОЙ ИНФОРМАЦИИ

В случае незапланированного отсутствия работника на рабочем месте передача парольно-ключевой информации возможна в случае служебной (оперативной) необходимости. Работник имеет право передать свои учетные данные от автоматизированного рабочего места, электронной почты, от ИСПД («…», «…», «…») (за исключением ограничений, установленных законодательством Российской Федерации в области защиты информации и коммерческой тайны) непосредственному руководителю (или лицу его замещающему) для решения оперативных задач в целях поддержания непрерывности рабочего процесса. Передача парольной информации должна осуществляться способом, отвечающим требованиям конфиденциальности, с учетом фактической ситуации внепланового отсутствия. По возвращению к должностным обязанностям работник обязан изменить пароль своей учетной записи. Ответственность за полученную парольно-ключевую информацию и ресурсы ею защищаемые возлагается на лицо, получившее такой доступ. В непредусмотренных настоящими требованиями случаях (например, невозможности установления связи с работником) допускается следующий механизм получения парольно-ключевой информации: работник, которому необходимо получить доступ к автоматизированному рабочему месту, почтовому ящику, ИСПД по согласованию с руководителем (или лицом его замещающим) обращается к директору МБОУ ДО ДЮЦ в рабочем порядке. Директор, установив возможность предоставления доступа, совместно с работником предоставляет доступ к автоматизированному рабочему месту посредством использования учетной записи Администратора. Передача парольно-ключевой информации (логина и/или пароля) третьим лицам запрещена.

4. РЕКОМЕНДАЦИИ

В целях усиления уровня защищенности при применении правил парольной защиты пользователям следует придерживаться следующих рекомендаций: вводе пароля, пользователю необходимо исключить возможность его

подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.):
− в случае прекращения полномочий пользователя (увольнение, либо переход на другую должность) производится немедленное удаление пароля сразу после окончания его последнего дня работы;
− срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение или переход на другую работу) администраторов информационной системы и других работников, которым по функциональным обязанностям были предоставлены полномочия по управлению системой парольной защиты;
− не используйте один и тот же пароль для доступа к учётным записям МБОУ ДО ДЮЦ и к другим ресурсам (например, доступ в интернет из дома, системам электронной коммерции и т.д.). По возможности не используйте один и тот же пароль для доступа к различным ресурсам внутри МБОУ ДО ДЮЦ. Например, используйте один пароль для прикладных программ и другой для администрирования ресурсов. Используйте различные пароли для учётных записей различных систем;
− не использовать ранее использованные пароли;
− не сообщайте никому свой пароль по телефону;
− не отправляйте свой пароль по электронной почте;
− не говорите о своём пароле рядом с посторонними;
− не упоминайте о содержимом пароля (например, «мой день рождения»);
− не указывайте свой пароль в анкетах или опросниках;
− не храните пароль в файле на компьютере, включая переносной, без шифрования;
− не используйте функцию «Запомнить пароль», например, в таких приложениях как Internet Explorer, FireFox, Google Chrome и т.д.;
− если кто-либо требует сообщить ваш пароль, сошлитесь на этот документ или попросите позвонить в Департамент по безопасности;
− если вы считаете, что учётная запись или пароль скомпрометированы, сообщите об этом в Департамент по безопасности и смените все пароли.

5. ОТВЕТСТВЕННОСТЬ

Работники МБОУ ДО ДЮЦ несут ответственность за сохранность парольной информации и соблюдение положений настоящей Политики безопасности. В случае выявления нарушений, к нарушителям могут быть применены меры дисциплинарного взыскания в соответствии с действующим законодательством Российской Федерации. Владельцы личных паролей должны быть ознакомлены под подпись с данной инструкцией и предупреждены об ответственности за разглашение парольной информации. Департамент по безопасности совместно с Департаментом информационных технологий организуют периодический контроль на рабочих местах

пользователей за правильностью обращения с личными паролями, соблюдением порядка их смены и хранения. В случае выявления нарушений установленного порядка работы с личными паролями или нарушения функционирования автоматизированного рабочего места пользователя требовать прекращения обработки информации, как для отдельных пользователей, так и в подсистеме в целом до выяснения их причин и замены личного пароля пользователя (пользователей).